

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
27. März 2003 (27.03.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 03/026229 A2

(51) Internationale Patentklassifikation⁷: **H04L 12/56**,
H04Q 11/04

(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): **SCHRODI, Karl**
[DE/DE]; Isarastrasse 2A, 82538 Geretsried (DE).

(21) Internationales Aktenzeichen: **PCT/DE02/03538**

(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGE-
SELLSCHAFT**; Postfach 22 16 34, 80506 München
(DE).

(22) Internationales Anmeldedatum:
20. September 2002 (20.09.2002)

(25) Einreichungssprache: **Deutsch**

(81) Bestimmungsstaaten (national): AE, AG, AL, AM, AT,
AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR,
CU, CZ, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH,
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,
LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,
MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG,
SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ,
VC, VN, YU, ZA, ZM, ZW.

(26) Veröffentlichungssprache: **Deutsch**

(30) Angaben zur Priorität:
101 46 349.9 20. September 2001 (20.09.2001) DE
101 61 546.9 14. Dezember 2001 (14.12.2001) DE

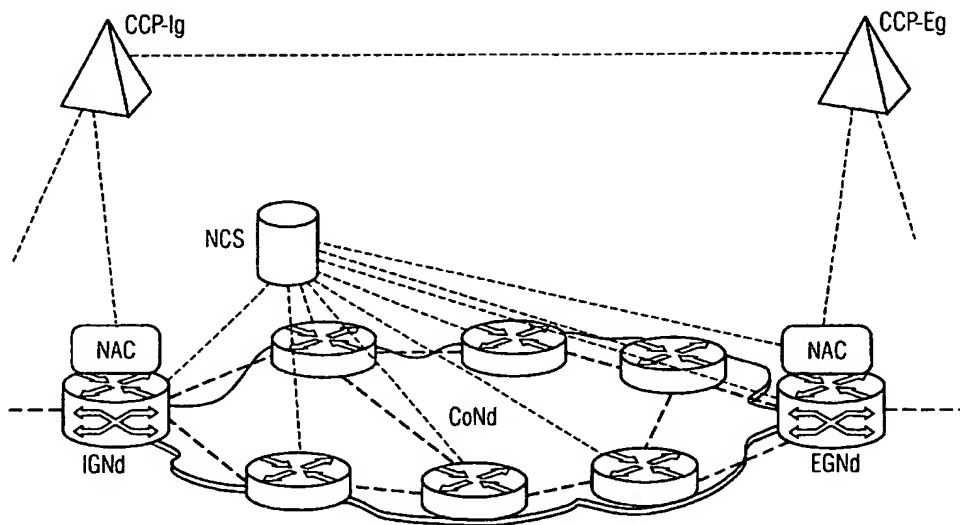
(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von
US): **SIEMENS AKTIENGESELLSCHAFT** [DE/DE];
Wittelsbacherplatz 2, 80333 München (DE).

(84) Bestimmungsstaaten (regional): ARIPO-Patent (GH,
GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),
eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ,

[Fortsetzung auf der nächsten Seite]

(54) Title: **TRAFFIC RESTRICTION FOR A NETWORK WITH QOS TRANSMISSION**

(54) Bezeichnung: **VERKEHRSBEGRENZUNG FÜR EIN NETZ MIT QOS NIVEAU ÜBERTRAGUNG**



(57) Abstract: The invention relates to a method, a network, a boundary node and a server for restricting the traffic in a packet-oriented, connectionless network for an efficient QoS transmission of prioritized data packets. According to the invention, reliability checks are carried out that include a reliability check with respect to the network input and the network output. The reliability checks allow to check whether resources meeting the requirements to transmission of a group of data packets of a priority class are available in the network. The invention allows to avoid resource shortages, especially at the network input and network output, thereby safeguarding QoS transmission.

[Fortsetzung auf der nächsten Seite]

WO 03/026229 A2

REPRODUCIBLE COPY



TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

Erklärungen gemäß Regel 4.17:

- hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die folgenden Bestimmungsstaaten AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD,

- Erfindererklärung (Regel 4.17 Ziffer iv) nur für US

Veröffentlicht:

- ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren, ein Netz, einen Randknoten und einen Server zur Verkehrsbegrenzung in einem paketorientierten, verbindungslosen Netz für eine effiziente Übertragung mit QoS Niveau von priorisierten Datenpaketen. Erfindungsgemäss werden Zulässigkeitsprüfungen durchgeführt, die eine auf den Netzeingang und den Netzausgang bezogene Zulässigkeitsprüfung umfassen. Durch die erfindungsgemässen Zulässigkeitsüberprüfungen wird überprüft, ob den Anforderungen bei der Übertragung einer Gruppe von Datenpaketen einer Prioritätsklasse entsprechende Ressourcen im Netz zur Verfügung stehen. Durch die Erfindung werden Ressourcenengpässe, insbesondere am Netzeingang und -ausgang, vermieden. Eine Übertragung mit QoS Niveau kann so gewährleistet werden.

Beschreibung

Verkehrsbegrenzung für ein Netz mit QoS Niveau Übertragung

Die Erfindung betrifft ein Verfahren, ein Netz, einen Randknoten und einen Server zur Verkehrsbegrenzung in einem paketorientierten, verbindungslosen Netz für eine effiziente Übertragung mit QoS Niveau von Datenpaketen zumindest einer Prioritätsklasse.

Die Integration von Telekommunikations- und Datendiensten führt zu einer Reihe von Anforderungen an Vermittlungstechnik und Netze. Um für Infotainment und Geschäftsverkehr gleichermaßen geeignet zu sein, sollten die benutzten Netze eine hohe Kapazität besitzen, Übertragung in Echtzeit zulassen, zuverlässig sein und ein hohes Maß an Sicherheit garantieren. Daneben steht als weitere Bedingung möglichst geringe Kosten.

Datendienste werden derzeit in großem Umfang über IP-Netze (auf dem Internet Protocol basierende Netze) abgewickelt, die paketorientiert und - auf der IP-Ebene - verbindungslos arbeiten. Fortschritte in der Router-Technologie haben zur Entwicklung von IP-Routern geführt, die hinsichtlich Kapazität des vermittelten Datenverkehrs und Verzögerungszeiten durch Warteschlangen prinzipiell Telekommunikationsdienste und bandbreitenintensive Dienste wie Video-on-Demand oder Video-konferenzen in Echtzeit ermöglichen.

Schwierigkeiten entstehen bei einem hohen Ausnutzungsgrad des IP-Netzes, bei dem die Verzögerungszeiten exponentiell anwachsen oder bei der übermäßigen Aggregation von Datenverkehr auf einzelnen Strecken, die dann als Flaschenhals wirken und die Übertragungsrate beschränken.

Ob dieser Schwierigkeiten ist es bei herkömmlichen IP-Netzen nicht in gewünschtem Umfang möglich, eine hohe Dienstqualität

- in der Literatur meist mit Quality of Service (QoS) bezeichnet - zu garantieren.

Weiterentwicklungen zielen darauf ab, bessere Zusagen hinsichtlich der Dienstqualität machen zu können, ohne die Vorteile der geringen Komplexität und Flexibilität des IP-Netzes einzubüßen.

Das Differentiated Services (Diff-Serv) Modell basiert auf der Beobachtung, dass die best-effort Behandlung von Datenpaketen im IP-Netz zu den oben genannten Schwierigkeiten bei der Garantie von Dienstqualität führt. Herkömmlich werden Datenpakete nach Möglichkeit schnell und vollständig übertragen, ohne dass Garantien hinsichtlich der Zuverlässigkeit und Sicherheit der Übertragung gegeben werden. Bei hoher Auslastung oder Überlastung des Netzes kommt es zur Beeinträchtigung der Dienstqualität durch Verzögerungen oder Verwurf von Datenpaketen.

Das Diff-Serv Konzept zielt auf eine bessere Dienstqualität für Dienste mit hohen Qualitätsanforderungen durch Einführung von Dienstklassen. Man spricht in diesem Zusammenhang auch häufig von einem CoS (class of service) Modell. Das Diff-Serv Konzept ist in den von der IETF veröffentlichten RFCs mit den Nummern 2474 und 2475 beschrieben. Die RFCs 2638 und 2998 behandeln weitere Aspekte des Konzepts. Im Rahmen des Diff-Serv Konzepts wird mit Hilfe eines DS (Differentiated Services) Feldes im IP Header der Datenpakete durch Setzen des DSCP (DS codepoint) Parameters eine Priorisierung des Paketverkehrs vorgenommen. Diese Priorisierung erfolgt mit Hilfe einer „per hop“ Ressourcenallokation, d.h. die Pakete erfahren bei den Knoten je nach der im DS Feld durch den DSCP Parameter festgelegten Dienstklasse (class of service) eine unterschiedliche Behandlung. Man verwendet in diesem Zusammenhang den Ausdruck per-hop behavior (PBH). Zum Beispiel werden im Zuge eines PBH höhere Dienstklassen hinsichtlich der Einreihung und

Abarbeitung von Warteschlangen bei den Knoten bevorzugt behandelt.

Die zentralen Elemente eines auf dem Diff-Serv Konzept beruhenden Netzes sind die DS Subnetze - in der englischsprachigen Literatur häufig als DS domain oder single routing domain bezeichnet - und die DS Randknoten. In vielen Fällen wird ein Subnetz dem Netz eines Diensteanbieters (service provider domain) entsprechen. Bei den DS Randknoten unterscheidet man zwischen DS Zugangsknoten (ingress nodes) und DS Ausgangsknoten (egress nodes). Datenpakete gelangen über einen DS Zugangsknoten in eine DS Subnetz und verlassen das Subnetz über einen DS Ausgangsknoten. Ein DS Randknoten kann dabei die Funktionalität eines DS Zugangsknoten für eingehenden Verkehr und eines DS Ausgangsknoten für ausgehenden Verkehr vereinen. Die Funktionalität der DS Randknoten umfasst die Auswahl von Datenpaketen entsprechend DSCP Parameter und das Markieren von Datenpaketen mit Hilfe von DSCP Parametern. Zudem besteht im DS Subnetz die Möglichkeit, mit Hilfe von Vorrichtungen zur Verwaltung und Kontrolle des Datenverkehrs (traffic conditioning) Steuermaßnahmen wie das Messen von Datenflüssen, die Verteilung von Datenpaketen auf Warteschlangen oder das Verwerfen von Datenpaketen vorzunehmen. Diese Steuermaßnahmen werden häufig in DS Zugangsknoten oder DS Ausgangsknoten vorgenommen. Im Rahmen von traffic conditioning können Datenpakete klassifiziert und mit einem für die entsprechende Dienstklasse vorgesehenes Verkehrsprofil (z.B. Bandbreite, Ressourcen) verglichen werden. Bei Abweichungen von dem Verkehrsprofil können Maßnahmen, wie das Einreihen in eine Warteschlange oder das Verwerfen von Datenpaketen, vorgenommen werden.

Typischerweise werden in einem DS Subnetz Flows oder Verbindungen priorisiert. Die Priorisierung erfolgt im DS Zugangsknoten für das entsprechende DS Subnetz gegebenenfalls durch Setzen bzw. Ändern des DSCP Parameters. Bei den Knoten innerhalb des Netzes (core nodes) wird der DSCP Parameter gelesen

und entsprechend der Priorisierung Ressourcen zugewiesen. Die Interpretation des DSCP Parameters und Ressourcenzuweisung der einzelnen inneren Knoten erfolgt unabhängig voneinander (per-hop behaviour). Bei dem Ausgangsknoten wird evtl. eine Änderung des DSCP Parameters beim Zugangsknoten rückgängig gemacht, d.h. der DSCP auf den ursprünglichen Wert zurückgesetzt. Auf diese Weise lässt sich der DSCP lokal, d.h. je nach Subnetz und dessen Eigenschaften, anpassen.

Das Diff-Serv Konzept vermeidet komplexe Reservierungsprozeduren von Pfaden oder Bandbreite und erlaubt Priorisierung von Datenverkehr. Bei einer Übertragung über mehrere Subnetze hinweg werden Dienstklassen mit Hilfe sogenannter Service Level Agreements (SLA) für die gesamte Übertragung festgelegt und von den einzelnen Subnetzen wie oben beschrieben im Rahmen des traffic conditionings umgesetzt. In der Praxis kommen aber temporäre und/oder lokale Engpässe beispielsweise durch Aggregierung von Datenverkehr auf einzelnen Strecken vor. Im Regelfall folgen Datenpakete mit dem gleichen Ziel von dem Moment an, in dem sie in einem Knoten zusammentreffen, derselben eingestellten Route. Bei Engpässen sorgt das Diff-Serv Konzept dafür, dass Datenpakete mit niedriger Priorität zuerst Verzögerungen oder Verwurf erfahren. Die Übertragungsqualität für die hoch priorisierten Datenpakete wird dadurch verbessert, aber Qualitätsstandards z.B. für Echtzeitübertragung können nicht garantiert werden. Im Rahmen des Diff-Serv Konzeptes gäbe es nur die Möglichkeit Übertragung mit QoS Niveau, d.h. eine Übertragung, bei der bestimmte Qualitätszusagen gegeben und eingehalten werden können, zu gewährleisten, wenn Verkehrsprofile mit einer so geringen Auslastung des Subnetzes eingestellt werden, dass Belastungsspitzen durch Reserve-Bandbreite abgefangen würde. Das wird aus wirtschaftlichen Gründen, d.h. wegen der daraus resultierenden geringen Netzauslastung, in der Regel nicht gemacht. Aus diesem Grunde spricht man im Zusammenhang mit dem Diff-Serv Konzept von einem CoS (class of service) Ansatz und nicht von einem QoS (quality of service) Ansatz.

Die Erfindung hat zur Aufgabe, eine effiziente Übertragung von Datenpaketen mit QoS Niveau für paketvermittelte, verbindungslos arbeitende Netze zu ermöglichen.

Die Aufgabe wird durch die Gegenstände der Ansprüche 1, 13, 18 und 20 gelöst.

Die Erfindung zielt auf ein effizientes QoS-fähiges Netz ab, das paketvermittelt und verbindungsorientiert arbeitet. Das Konzept für das Netz beinhaltet folgende drei Überlegungen:

- Eine hohe Effizienz erfordert Flexibilität bei der Wahl der Wege von Datenpaketen bzw. bei deren Verteilung. Mit einer dynamischen Änderung bzw. Anpassung von Wegen kann z.B. der Entstehung von Ressourcenengpässen entgegengewirkt werden.
- Eine hohe Komplexität lässt sich verhindern, indem lokal, z.B. jeweils vom betroffenen Router, Entscheidungen (z.B. über Wege, Warteschlangen, Verwurf von Datenpaketen etc.) getroffen werden. Nicht-lokale Zustände bzw. Reservierung von Wegen wird vermieden. Entscheidungen über Wege können je nach Datenpaket oder je nach Verbindung bzw. Flow getroffen werden. Dabei ist die Verteilung einzelner Datenpakete am flexibelsten.
- Um QoS zu garantieren, bedarf es strikter Grenzen und einer Überwachung hinsichtlich der Auslastung des Netzes.

Die vorliegende Patentanmeldung behandelt den dritten Aspekt.

Durch die erfindungsgemäßen Zulässigkeitsüberprüfungen soll überprüft werden, ob den Anforderungen bei der Übertragung einer Gruppe von Datenpaketen einer Prioritätsklasse korrespondierende Ressourcen im Netz zur Verfügung stehen. Erfindungsgemäß werden für durch das Netz zu leitende Gruppen von Datenpaketen zumindest einer Prioritätsklasse Zulässigkeitsprüfungen durchgeführt. Diese Zulässigkeitsprüfungen umfassen

auf den Netzeingang und am Netzausgang bezogene Zulässigkeitsprüfungen, die auch am Netzeingang und am Netzausgang durchgeführt werden können. Nur bei Gruppen von Datenpaketen, für die alle Zulässigkeitsprüfungen positiv ausfallen, wird die Übertragung mit der Prioritätsklasse der Datenpakete zugelassen. Dagegen wird mit Gruppen von Datenpaketen, bei denen eine der Zulässigkeitsprüfungen negativ ausfällt, anders verfahren (Anspruch 1).

Eine Gruppe von Datenpaketen kann dabei durch die Datenpakete eines Verkehrsstroms oder durch die an einem physikalischen Port, z.B. bei einem Netzzugang, aggregierten Datenpakete gegeben sein (Anspruch 2). Ein Verkehrsstrom entspricht beispielsweise einem Flow, umfasst die Datenpakete einer Verbindung oder umfasst Datenpakete mit einer identischen Adressinformation, wie z.B. alle Datenpakete mit derselben Quelle oder demselben Ziel (Anspruch 3).

Um eine Übertragung mit QoS Niveau zu gewährleisten, muss eine Überlastung der Gesamtkapazität des Netzes und das Auftreten von Ressourcenengpässen verhindert werden. In diesem Sinne können bei den Zulässigkeitsprüfung der zu übertragenden Gruppen von Datenpaketen nach Parametern wie z.B. mittlere Daten- und/oder Paketrate, Spitzenrate, etc. bewertet werden, und es kann überprüft werden, ob für die Übertragung der Verkehrsströme mit der angeforderten Dienstqualität ausreichend Übertragungskapazität zur Verfügung steht. Zudem wird durch die Zulässigkeitsprüfungen sichergestellt, dass eingangs- sowie ausgangsseitig genug Ressourcen (z.B. Bandbreite, Warteschlangenkapazität, ...) zur Verfügung stehen (Anspruch 4). Die Überprüfung kann abhängig von der Prioritätsklasse der Datenpakete oder abhängig von dem Verkehr mit gleicher oder höherer Priorität erfolgen (Anspruch 5). Beispielsweise könnte ohne Zulässigkeitsprüfung der ausgangsseitigen Ressourcen von mehreren Eingängen des Netzes zum selben Ausgang übertragen werden und so bei dem Ausgang ein Engpass entstehen. Qualitätsgarantien könnten dann nicht eingehalten werden, son-

dern bestenfalls nur - wie bei dem Diff-Serv Konzept - Zusagen hinsichtlich der priorisierten Behandlung von Verkehrsströmen.

Als Kriterium für ein positives Ergebnis der Zulässigkeitsprüfungen kann z.B. ein Schwellenwert dienen, der abhängig von der Kapazität von dem jeweils benutzten Netzeingang und -ausgang, der Gesamtkapazität des Netzes, der gewünschten Qualität bzw. Prioritätsklasse etc. bestimmt wird. Beispielsweise werden für eine mit einer Priorität zu übertragende Gruppe von Datenpaketen Verkehrsparameter wie die mittlere Daten- und/oder Paketrate und die Spitzenrate angemeldet (Anspruch 7). Zudem kann die gewünschte Prioritätsklasse angemeldet werden. Alternativ wird die Prioritätsklasse auf Grund von Parametern bzw. Anforderungen wie maximale Verlustrate und Echtzeitübertragung bestimmt.

Denkbar ist auch, dass es für jede Prioritätsklasse mehrere Schwellenwerte auf Basis unterschiedlicher Bewertungsparameter gibt, die alle separat oder in entsprechenden Abhängigkeiten voneinander einzuhalten sind. Bei einem negativen Ergebnis der Zulässigkeitsprüfungen kann die Übertragung der Gruppe von Datenpaketen abgewiesen werden (Anspruch 6) oder die Übertragung mit einer niedrigeren Priorität oder nicht priorisiert erfolgen.

Auf Grund der Zulässigkeitsprüfungen kann nach Maßgabe der angeforderten Qualitätsmerkmale eine Reservierung von Ressourcen (z.B. Bandbreite, Warteschlangen) vorgenommen werden (Anspruch 8). Diese Reservierung wird im Regelfall den betroffenen Netzzugang und -ausgang sowie die Gesamtnetzbelastung (z.B. Kapazität, Behandlung bei Warteschlangen entsprechend Priorisierung) betreffen.

Die Einhaltung der zentralen, für die jeweiligen Verkehrsströme angemeldete Verkehrsparameter wie z.B. der Übertragungsrates sollte nach Möglichkeit überwacht werden, um die

Einhaltung der Grenzwerte bzw. Schwellenwerte für die Auslastung des Netzes zu garantieren (Anspruch 9). Die Überwachungsfunktion – die englischen Begriffe traffic enforcement und policing finden sich häufig in der Literatur dafür – wird sinnvollerweise die bei der Anforderung der Qualitätsmerkmale angegebenen Verkehrsparameter mit den tatsächlichen Verkehrsparameter des entsprechenden Verkehrsstroms vergleichen.

Nicht angemeldete Datenpakete können ausgeblockt werden (Anspruch 10). Am Netzeingang können zudem bekannte traffic shaping Mechanismen wie leaky bucket oder token bucket zum Einsatz kommen. Mögliche Überlastabwehrmaßnahmen sind z.B.

- Der Verwurf von Datenpaketen
- Das Markieren von Datenpaketen
- Das Puffern von Datenpaketen
- Das Umschalten oder Blockieren des Verkehrsstroms
- Das Umsetzen der die Vereinbarung verletzenden Datenpakete oder des gesamten zugehörigen Datenstroms auf eine niedrigere Prioritätsklasse oder Behandlung entsprechend des best effort Ansatzes

Eine Übertragung mit QoS Niveau von Verkehrsströmen mit entsprechender Prioritätsklasse bzw. Verkehrsklasse setzt eine entsprechende Behandlung der Prioritätsklasse voraus. Es ist sinnvoll, nur einen Teil der Gesamtkapazität mit priorisiertem Verkehr auszulasten. Der andere Teil der Kapazität des Netzes wird dann mit nicht-priorisiertem Verkehr ausgelastet. Diese nicht-priorisierte Verkehr kann dann entsprechend dem best-effort Prinzip behandelt werden (Anspruch 12). Die Zulässigkeitsüberprüfungen können dann auf den priorisierten Verkehr beschränkt werden (Anspruch 11). Durch diese Beschränkung des priorisierten Verkehrs wird sichergestellt, dass die Kapazität des Netzes voll ausgelastet werden kann, ohne dass sich Belastungsspitzen negativ auf den priorisierten Verkehr auswirken. Das Qualitätsniveau, mit der nicht-priorisierter Verkehr übertragen wird, wirkt dann quasi als Puffer für den priorisierten Verkehr. Eine mögliche Vorgehensweise, Grenzen für die Auslastung mit priorisiertem Verkehr zu setzen, ist,

für jede Prioritätsklasse eine feste maximale prozentuale Auslastung für den Verkehr mit gleicher oder höherer Prioritätsklasse anzugeben. Beispielsweise könnte man in einem Netz mit zwei Prioritätsklassen für Verkehr mit der höheren Verkehrsklasse die Grenze auf eine Auslastung mit 30% setzen und die Grenze für Verkehr mit der höheren oder niedrigeren Prioritätsklasse auf 60% festlegen. Für nicht-priorisierten Verkehr bliebe dann eine minimale Kapazität von 40%.

Bei der Übertragung von Datenpaketen können so prioritätsklassenspezifisch Qualitätsmerkmale garantiert werden, die eine Übertragung mit QoS Niveau ermöglichen. Das erfindungsgemäße Konzept geht dabei von der Beobachtung aus, dass sich eine geeignete Dienstqualität (QoS) am jeweiligen Dienst zu orientieren hat. Z.B. können menschliche Sinnesorgane in einem gewissen Rahmen unvollständige Information verarbeiten, ohne dass es zu einem subjektiven Qualitätsverlust kommt. Für die interaktive Steuerung von Maschinen (z.B. Fernsteuerung von Robotern) sind die Anforderungen unter Umständen deutlich höher. Entsprechend strengere Kriterien sollten dann angewandt werden. Dienstabhängig können deshalb Kriterien bzw. Grenzen definiert werden, die eine QoS Niveau Übertragung gewährleisten. Bei paketorientierter Übermittlung betreffen diese Kriterien u.a.

- Art und Umfang möglicher Informationsverluste
- Feste und/oder variable Verzögerungen
- Die zeitliche Konsistenz (Reihenfolge) der Informationen.

Erfindungsgemäß ist das Netz mit Mitteln zur Durchführung einer Zulässigkeitsprüfung am Netzeingang und am Netzausgang für die Übertragung eines durch das Netz zu leitenden Gruppe von Datenpaketen einer Prioritätsklasse ausgestattet (Anspruch 13). Es kann im Sinne einer Übertragung von priorisierten Datenpaketen mit QoS Niveau dimensioniert werden. Die Dimensionierung kann dabei nach Maßgabe von Grenzwerten für QoS bestimmende Kriterien bzw. Faktoren erfolgen (Anspruch 14). Je nach Dienst können maximale Werte für die statisti-

sche Wahrscheinlichkeit angegeben werden, mit der die Grenzwerte für die QoS bestimmenden Faktoren überschritten werden können, ohne dass es zu einer signifikanten Qualitätseinbuße kommt. Diese maximalen Werte für die statistische Wahrscheinlichkeit können in die Dimensionierung des Netzes einfließen (Anspruch 15).

Durch das Einhalten von Auslastungsgrenzen für das Netz - möglicherweise im Rahmen einer dienstspezifisch vorgegebenen statistischer Wahrscheinlichkeit - und der Beschränkung des priorisierten Verkehrs sowie durch eine gute Verteilung des Verkehrs und der Limitierung des Verkehrs an den Zugängen und Ausgängen des Netzes bzw. den physikalischen Ports können statistische Werte für die Qualitätsverlustfaktoren angegeben werden. Mit Hilfe dieser statistischen Werte und ihrer Varianz lassen sich QoS Dienste garantieren.

In vielen Fällen ist es sinnvoll, wenn das Netz einer single routing domain oder dem Netz eines Diensteanbieters (service provider domain) entspricht (Anspruch 16). Auf diese Weise können die Funktionen der Zulässigkeitsprüfungen und der Überwachung einfacher in das Netz integriert werden. Vertrauliche Leistungsdaten des Netzes brauchen nicht nach außen gegeben werden. Bei der Übertragung über mehrere single routing domains oder Dienstanbieterernetze ist durch die Garantie durch die Netzverwaltung in den jeweiligen Netz und Überprüfung der Netzzu- und -abgänge sichergestellt, dass QoS Niveau Übertragung über mehrere, miteinander verbundene erfindungsgemäße Netze und gegebenenfalls an einen an ein erfindungsgemäßes Netz angeschlossenen Host möglich ist. Ein Internet mit QoS Niveau Übertragung kann so aus erfindungsgemäß funktionieren den Netzen, die z.B. jeweils eine single routing domain umfassen, aufgebaut werden. Dabei können wie im Rahmen des herkömmlichen Internets IP basierte Netze verwendet werden (Anspruch 17), die z.B. nicht priorisierten Verkehr entsprechend dem best-effort Prinzip übertragen.

Eine wichtige Rolle kommt dabei den Randknoten der Netze zu, über die der Datenverkehr in das jeweilige Netz gelangt bzw. dieses wieder verlässt. Durch die Zulässigkeitsprüfungen für priorisierten Verkehr hinsichtlich der Ressourcen am Netzeingang und am Netzausgang kann sichergestellt werden, dass bei dem Übergang von Netzen die quality of service erhalten bleibt. Für die Zulässigkeitsprüfung können Randknoten mit Mitteln zur Durchführung der Zulässigkeitsprüfungen am Netzeingang oder am Netzausgang ausgestattet sein (Anspruch 18). Die Randknoten können zudem Mittel für die Überwachungsfunktionen aufweisen (Anspruch 19). Es kann auch alternativ oder komplementär zu der Bereitstellung der Funktionen in Randknoten ein Server mit Mittel für die Zulässigkeitsprüfungen (Anspruch 20) und evtl. für die Überwachung (Anspruch 21) im Netz platziert werden.

Im folgenden werden zwei Varianten des Erfindungsgegenstands im Rahmen als Ausführungsbeispiels dargestellt. Es zeigen

Fig. 1: System mit Datenübertragung über ein erfindungsgemäßes Netz

Fig. 2: Erfindungsgemäßes Netz

Fig. 3: Schematische Darstellung verschiedener Wege für das Routing zweier Flows in einem erfindungsgemäßen Netz

Fig. 4: Schematische Darstellung verschiedener Wege für das Routing zweier Flows mit gleichen Ziel in einem erfindungsgemäßen Netz

Der Anschaulichkeit wegen sei angenommen, dass die Erfindung im Rahmen eines Telefonats über ein IP Netz IPN – man spricht hier von Voice over IP (VoIP) zur Anwendung komme. Bei diesem IP Netz IPN kann es sich z.B. um eine Single Routing Domain des Internets handeln. Telefonate unterliegen Echtzeitanforderungen. Der zugehörige Datenverkehr wird deshalb priori-

siert. Sinngemäß ist der Erfindungsgegenstand analog für alle anderen Dienste, bei denen eine Priorisierung des Datenverkehrs notwendig ist, anwendbar. Beispiele für solche Dienste sind Video-on demand, Web-Konferenzen, Multimediaanwendungen etc.

In Figur 1 ist schematisch ein System mit VoIP Übertragung dargestellt. Über Zugangsnetze AN-A und AN-B (AN: für Access Network) sind die Telekommunikations-Endgeräte TLN-A und TLN-B an ein öffentliches Netz angeschlossen, das das IP Netz IPN umfasst. Im Rahmen der zwei Varianten des Ausführungsbeispiels wird angenommen, dass vom Endgerät TLN-A eine Verbindung zu dem Endgerät TLN-B zwecks eines Telefonats aufgebaut wird. Dabei wird zwischen Dienstebene SL (SL: für service level) und Netzwerkebene (NL: für network level) unterschieden, was in der Figur durch eine durchbrochene Linie kenntlich gemacht ist. Auf der Dienstebene SL findet die Signalisierung SIG(VA,DS) (SIG(VA,DS) für: Signalisierung von Verbindungsaufbau und Dienststeuerung) des Verbindungsaufbaus und der Dienststeuerung statt. Zu diesem Zwecke sind Steuervorrichtungen CCP-A und CCP-B (CCP: für Call Control Point) z.B. Media Gateway Controller oder Vermittlungsanlagen mit den Zugangsnetzen AN-A und AN-B der Endgeräte TLN-A und TLN-B verbunden. Die Übertragung von Nutzdaten erfolgt auf der Netzwerkebene NL und führt zumindest zum Teil über das erfindungsgemäße Netz IPN (IPN: für IP Net). Das Netz IPN arbeitet paketorientiert und verbindungslos. Nutzdatenpakete, die im Rahmen des Telefonats von dem Endgerät TLN-A zu dem Endgerät TLN-B übertragen werden, gelangen über den Randknoten IgNd (IgNd: für ingress node) in das Netz IPN und verlassen es wieder über den Randknoten EgNd (EgNd: für egress node).

Im Zuge des Verbindungsaufbaus auf der Dienstebene SL wird von Endgerät TLN-A über das Zugangsnetz AN-A an die Steuereinrichtung CCP-A der Verbindungswunsch signalisiert. Das Endgerät TLN-A wird authentifiziert, beispielsweise anhand einer Namens- oder Adressinformation. Anschließend wird das

gerufene Endgerät TLN-B bzw. die zugeordnete Steuereinrichtung CCP-B identifiziert und lokalisiert. Üblicherweise wird eine Verbindungsaufbaunachricht von der Steuereinrichtung CCP-A an die Steuereinrichtung CCP-B übermittelt. In der Steuereinrichtung CCP-B werden relevante Informationen extrahiert und bei dem Zugangsnetz AC-B die Verfügbarkeit des Endgeräts TLN-B überprüft sowie relevante Informationen abgefragt. Die Verbindungsaufbaunachricht wird schließlich von der Steuereinrichtung CCP-B zur Steuereinrichtung CCP-A quittiert und die für die Verbindung erforderlichen Informationen wie z.B. Adressinformationen des Endgeräts TLN-B übermittelt. Anschließend kann der Verbindungsaufbau auf der Dienstebene SL abgeschlossen werden. Bei erfolgreichen Verbindungsaufbau können auf der Netzwerkebene NL dann Nutzdaten ausgetauscht werden.

Bei dem gewählten Beispiel werden als Nutzdaten Sprachinformationen in Echtzeit, d.h. mit QoS Niveau ausgetauscht. Für die Übertragung mit QoS Niveau werden erfindungsgemäß Zulässigkeitsprüfungen durchgeführt. Im Rahmen dieser Zulässigkeitsüberprüfungen findet Signalisierung statt, z.B. bei der Übermittlung der gewünschten Qualitätsanforderungen, zur Übermittlung des Resultats der Zulässigkeitsprüfungen etc. Im folgenden wird diese Signalisierung als QoS-Signalisierung bezeichnet. Es werden zwei Varianten unterschieden, je nachdem, ob die QoS-Signalisierung im Rahmen der Zulässigkeitsprüfungen auf der Dienstebene SL oder der Netzwerkebene NL durchgeführt wird.

Bei einer QoS-Signalisierung auf der Dienstebene SL kann das erfindungsgemäße Verfahren wie folgt ablaufen: Über Steuereinrichtungen der Dienstebene, CCP-Ig und CCP-Eg, werden die Randknoten IgNd und EgNd identifiziert, über die die Nutzdaten als Nutzdaten-Pakete übertragen werden. Die in Figur 2 dargestellten Steuereinrichtungen CCP-Ig und CCP-Eg können, aber müssen nicht mit den den Zugangsnetzen AN-A und AN-B zugeordneten Steuervorrichtungen CCP-A und CC-P identisch sein.

In der Regel wird bei Ferngesprächen auf der Dienstebene SL eine Mehrzahl von Steuervorrichtungen bei der Signalisierung beteiligt sein. Diese Steuervorrichtungen haben dann direkten Zugriff nur auf einen Abschnitt oder ein Teilnetz der gesamten Übertragungsstrecke für die Nutzdaten. Die Steuereinrichtungen CCP-Ig (CCP-Ig: für call control point at ingress node) und CCP-Eg (CCP-Eg: für call control point at egress node) sind dadurch gekennzeichnet, dass sie mit den Randknoten IgNd und EgNd kommunizieren. Die beiden Steuervorrichtungen CCP-Ig und CCP-Eg können dabei auch zusammenfallen.

In Figur 2 sind weitere Randknoten eingezeichnet. Nicht einzeln dargestellt sind die inneren Knoten CoNd (CoNd: für core node). Es ist zudem ein Kontrollserver NCS (NCS: für network control server) gezeigt, durch den Netzwerk-Management Aufgaben wahrgenommen werden.

Die erfindungsgemäßen Zulässigkeitsprüfungen NAC (NAC: für network admission control) hinsichtlich Netzeingang und Netzausgang finden z.B. in den Randknoten IgNd bzw. EgNd statt. Durch die Steuereinrichtungen CCP-Ig und CCP-Eg der Dienstebene SL werden den Randknoten IgNd und EgNd die Anforderungen für das VoIP-Telefonat zwischen den Endgeräten TLN-A und TLN-B übermittelt. Die Anforderungen können neben den relevanten Verkehrsparametern, wie der Bandbreite und den QoS-Anforderungen zusätzliche Parameter hinsichtlich Zuverlässigkeit, Sicherheit, etc. umfassen. Das Ergebnis der Zuverlässigkeitsprüfungen an den Netzgrenzen wird den Steuervorrichtungen CCP-A und CCP-B signalisiert. Abhängig von den Ergebnissen der Zulässigkeitsprüfungen wird A-seitig die Übertragung der Nutzdaten freigegeben oder abgeblockt und evtl. eine alternative Route für die Nutzdatenübertragung gesucht (in der englischsprachigen Literatur auch als Bearer Redirection bekannt). Die Zulässigkeitsprüfungen können nach oder während des Verbindungsaufbaus auf der Dienstebene SL stattfinden. Bei Zulässigkeitsprüfungen während des Verbindungsaufbaus

kann evtl. bei einem negativen Ergebnis der Verbindungsaufbau abgebrochen werden.

Bei QoS-Signalisierung auf der Netzwerkebene NL werden die Zulässigkeitsprüfungen erst nach dem Verbindungsaufbau auf der Dienstebene SL angestoßen. Nach erfolgreichen Verbindungsaufbau auf der Dienstebene SL wird die QoS-Signalisierung auf der Netzwerkebene NL freigegeben und es werden die relevanten Informationen, wie z.B. B-seitige Adressinformationen übergeben. Das kann durch eine entsprechende Nachricht von der Steuervorrichtung CCP-A an eine im Zugangsnetz AC-A positionierte Vorrichtung, z.B. Mediagateway, erfolgen. Zur QoS-Signalisierung kann auch von der Dienstebene SL z.B. von der Steuervorrichtung CCP-A eine Programmstruktur, z.B. ein Java-Applet der Vorrichtung im Zugangsnetz zur Verfügung gestellt werden. Mit Hilfe der im Rahmen des Dienstaufbaus auf der Dienstebene erfragten Adressinformationen und gegebenenfalls mit Hilfe der heruntergeladenen Programmstruktur wird auf der Netzwerkebene eine Signalisierungsnachricht an das B-seitige Endgerät TLN-B bzw. das B-seitige Zugangsnetz AN-B gesendet. Durch diese und evtl. weitere Signalisierungsnachrichten werden die Randknoten IgNd und EgNd lokalisiert und in den Randknoten die Zulässigkeitsprüfungen veranlasst. Die Ergebnisse der Zulässigkeitsprüfungen werden anschließend durch Nachrichten auf der Netzwerkebene NL an das A-seitige Zugangsnetz AN-A bzw. den A-seitigen Teilnehmer TLN-A signalisiert.

Zusätzlich zu den Zulässigkeitsprüfungen hinsichtlich Netzeingang und -ausgang wird eine Zulässigkeitsprüfung betreffend die Gesamtkapazität des Netzes vorgenommen. Diese Zulässigkeitsprüfung kann z.B. auch in einem der Randknoten IgNd bzw. EgNd, verteilt auf beide Randknoten IgNd und EgNd oder in einem dafür im Netz vorgesehenen Server erfolgen.

Figur 3 zeigt eine schematische Darstellung verschiedener Wege für das Routing zweier Flows in einem erfindungsgemäßen

Netz. Die Grenze des Netzes ist durch eine gepunktete Linie dargestellt. Netzknoten sind durch Kreise wiedergegeben, wobei die Kreise, die Rangknoten repräsentieren, die gepunktete Linie schneiden. Mit Hilfe von Pfeilen sind mögliche Wege für Flows dargestellt. Die gestrichelten Pfeile betreffen mögliche Wege für einen Flow, der bei dem Rangknoten C in das Netz eintritt und zu dem Randknoten D übertragen wird, wo die Datenpakete des Flows das Netz wieder verlassen. Durch durchgezogene Pfeile sind mögliche Wege für einen Flow dargestellt, der von dem Randknoten A zu dem Randknoten B geleitet wird. Bei den meisten inneren Knoten gibt es mehr als eine Alternative bzw. Verzweigungen für Weg des Flows. Im folgenden werden für einen bestimmten Flow die verschiedenen alternativen möglichen Wegabschnitte von einem inneren Knoten zu dem nächsten Knoten, d.h. für den „next hop“, als Verzweigungsfächer des Flows bei dem entsprechenden inneren Knoten bezeichnet. Bei inneren Knoten, die auf möglichen Wegen beider Flows liegen, ist angegeben, ob die Verzweigungsfächer der Flows identisch i, teilweise disjunkt t oder disjunkt d sind.

Die möglichen Wege bestimmen sich aus Parametern des Netzes, wie Topologie, Kapazität der einzelnen Wegabschnitte, Verzögerungszeiten etc. Die Entscheidungen über den Arm des Wegesfächers, über den ein Paket oder eine Gruppe von Paketen weiter übertragen wird, wird lokal in Abhängigkeit der momentan gültigen Verkehrsparameter getroffen. Auf diese Weise wird eine relativ gleichmäßige Auslastung des Netzes erreicht und Belastungsengpässe werden vermieden.

In Figur 4 unterscheidet sich von Figur 3 dadurch, dass nun beide Flows das Netz bei dem Randknoten B verlassen. Bei den inneren Knoten, die auf möglichen Wegen beider Flows liegen, sind die Verteilungsfächer beider Flows identisch, was ein i bei den Knoten verdeutlicht ist. Die Verteilungsfächer könnten im Rahmen von Verkehrssteuerung, bzw. traffic shaping, auch voneinander abweichen. Sie werden aber für Flows mit dem gleichen Ziel zumindest weitgehend identisch sein. Durch die

erfindungsgemäßen Zulässigkeitsprüfungen wird erreicht, dass der Randknoten B und die inneren Knoten, die dem Randknoten topologisch benachbart sind, nicht durch die ankommenden Datenpakete beider Flows überlastet werden. Wenn beide Flows nicht mit den angemeldeten Parametern übertragen werden können, wird beispielsweise einer nicht zugelassen. Bei der Beschränkung der Zulässigkeitsüberprüfungen auf den Netzeingang könnte es in der Konstellation von Figur 4 zu einem Engpass bei dem Randknoten B kommen, der QoS Garantiezusagen im Wege stünde.

Patentansprüche

1. Verfahren zur Verkehrsbegrenzung in einem paketorientierten, verbindungslosen Netz für eine effiziente Übertragung mit QoS Niveau von Datenpaketen zumindest einer Prioritätsklasse, bei dem
 - für eine Gruppe von durch das Netz zu leitenden Datenpaketen einer Prioritätsklasse Zulässigkeitsprüfungen durchgeführt werden,
 - die Zulässigkeitsprüfungen eine auf den Netzeingang und auf den Netzausgang bezogene Zulässigkeitsprüfung umfassen, und
 - die Übertragung der Gruppe von Datenpaketen mit der angeforderten Priorität nur zugelassen wird, wenn die Zulässigkeitsprüfungen positiv ausfallen.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet,
 - dass die Gruppe von Datenpaketen durch die Datenpakete eines Verkehrsstroms oder durch die an einem Port aggregierten Datenpakete der Prioritätsklasse gegeben ist.
3. Verfahren nach Anspruch 2, dadurch gekennzeichnet,
 - dass der Verkehrsstrom durch einen Flow gegeben ist, einer Verbindung zugeordnet ist oder Datenpakete mit einer gemeinsamen Adressinformation umfasst.
4. Verfahren einem der vorhergehenden Ansprüche, dadurch gekennzeichnet,
 - dass im Rahmen der Zulässigkeitsprüfungen der Auslastungsgrad betreffend die Gesamtkapazität des Netzes und die zur Verfügung stehende Bandbreite der bei der Übermittlung der Gruppe von Datenpaketen zu verwendenden eingangs- und ausgangsseitigen Netzzugänge berücksichtigt wird.
5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet,

- dass im Rahmen der Zulässigkeitsprüfungen der Auslastungsgrad des Netzes und der bei der Übermittlung der Gruppe von Datenpaketen zu verwendenden eingangs- und ausgangsseitigen Netzzugänge der Verkehr der Prioritätsklasse des zu übertragenden Verkehrsstroms oder/und der Verkehr einer Prioritätsklasse, die höher oder gleich der Prioritätsklasse der Gruppe von Datenpaketen ist, berücksichtigt wird.

6. Verfahren einem der vorhergehenden Ansprüche, dadurch gekennzeichnet,

- dass bei einem negativen Ergebnis der Zulässigkeitsüberprüfungen die Gruppe von Datenpaketen abgewiesen wird.

7. Verfahren einem der vorhergehenden Ansprüche, dadurch gekennzeichnet,

- dass für die durch das Netz zu leitenden Gruppe von Datenpaketen Verkehrsparameter in dem Netz angemeldet werden, die eine Information betreffend die benötigten Übertragungsressourcen umfassen.

8. Verfahren nach Anspruch 7, dadurch gekennzeichnet,

- dass nach Maßgabe der angemeldeten Verkehrsparameter eine Reservierung von Übertragungsressourcen vorgenommen wird.

9. Verfahren nach Anspruch 7, dadurch gekennzeichnet,

- dass während der Übertragung des Verkehrsstroms überprüft wird, dass die angemeldeten Verkehrsparameter eingehalten werden.

10. Verfahren nach Anspruch 7, dadurch gekennzeichnet,

- dass nicht angemeldete Datenpakete ausgeblockt/verworfen werden.

11. Verfahren einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

- dass Zulässigkeitsprüfungen nur für priorisierten Verkehr durchgeführt wird.

12. Verfahren einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

- dass nicht priorisierte Datenpakete mit best-effort Qualität übertragen werden.

13. Paketorientiertes, verbindungsloses Netz zur Datenübertragung,

- mit Mitteln zur Durchführung einer Zulässigkeitsprüfung am Netzeingang und am Netzausgang für die Übertragung einer durch das Netz zu leitenden Gruppe von Datenpaketen einer Prioritätsklasse.

14. Netz nach Anspruch 13,

dadurch gekennzeichnet,

- dass das Netz nach Maßgabe von Grenzwerten für QoS bestimmende Faktoren dimensioniert ist.

15. Netz nach Anspruch 14,

dadurch gekennzeichnet,

- dass das Netz nach Maßgabe von maximalen Werten für die statistische Wahrscheinlichkeit dimensioniert ist, mit der die Grenzwerte der QoS bestimmenden Faktoren überschritten werden.

16. Netz nach einem der Ansprüche 13 bis 15,

dadurch gekennzeichnet,

- dass das Netz einer Single Routing Domain entspricht.

17. Netz nach einem der Ansprüche 13 bis 16,

dadurch gekennzeichnet,

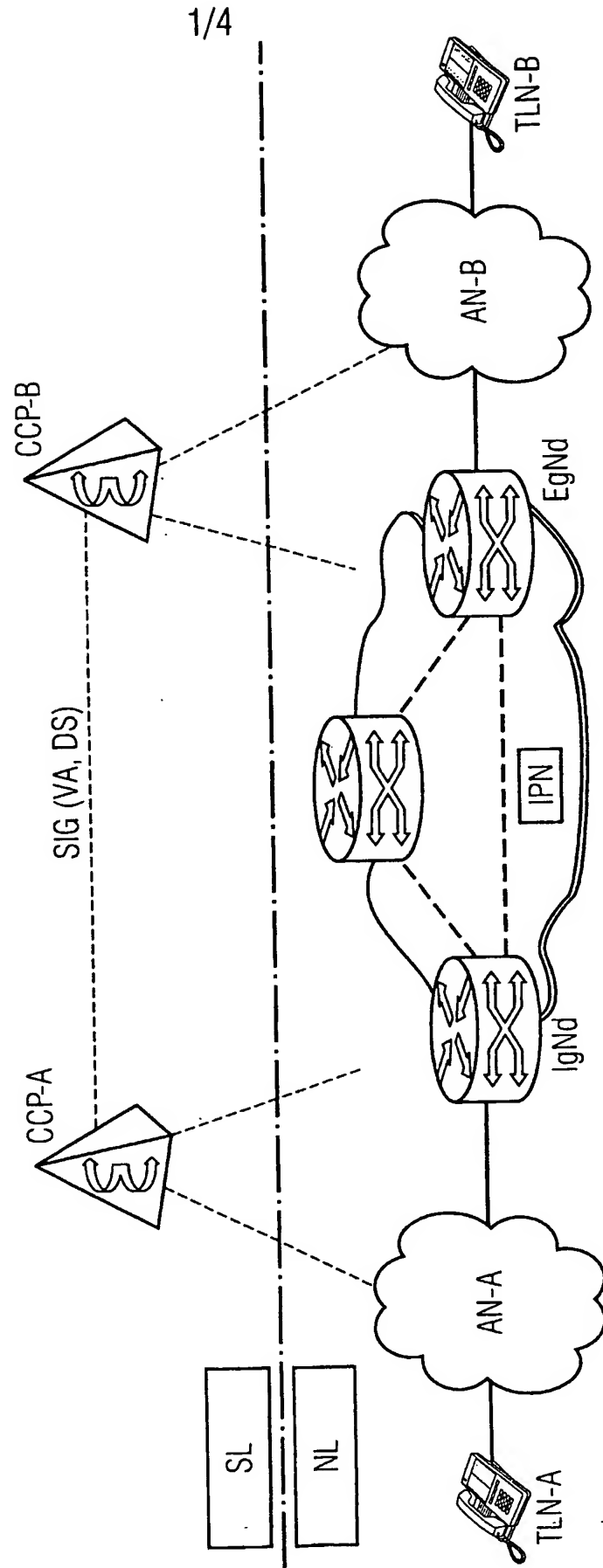
- dass eine Datenübertragung über das Netz mit Hilfe des IP Protokolls vornehmbar ist.

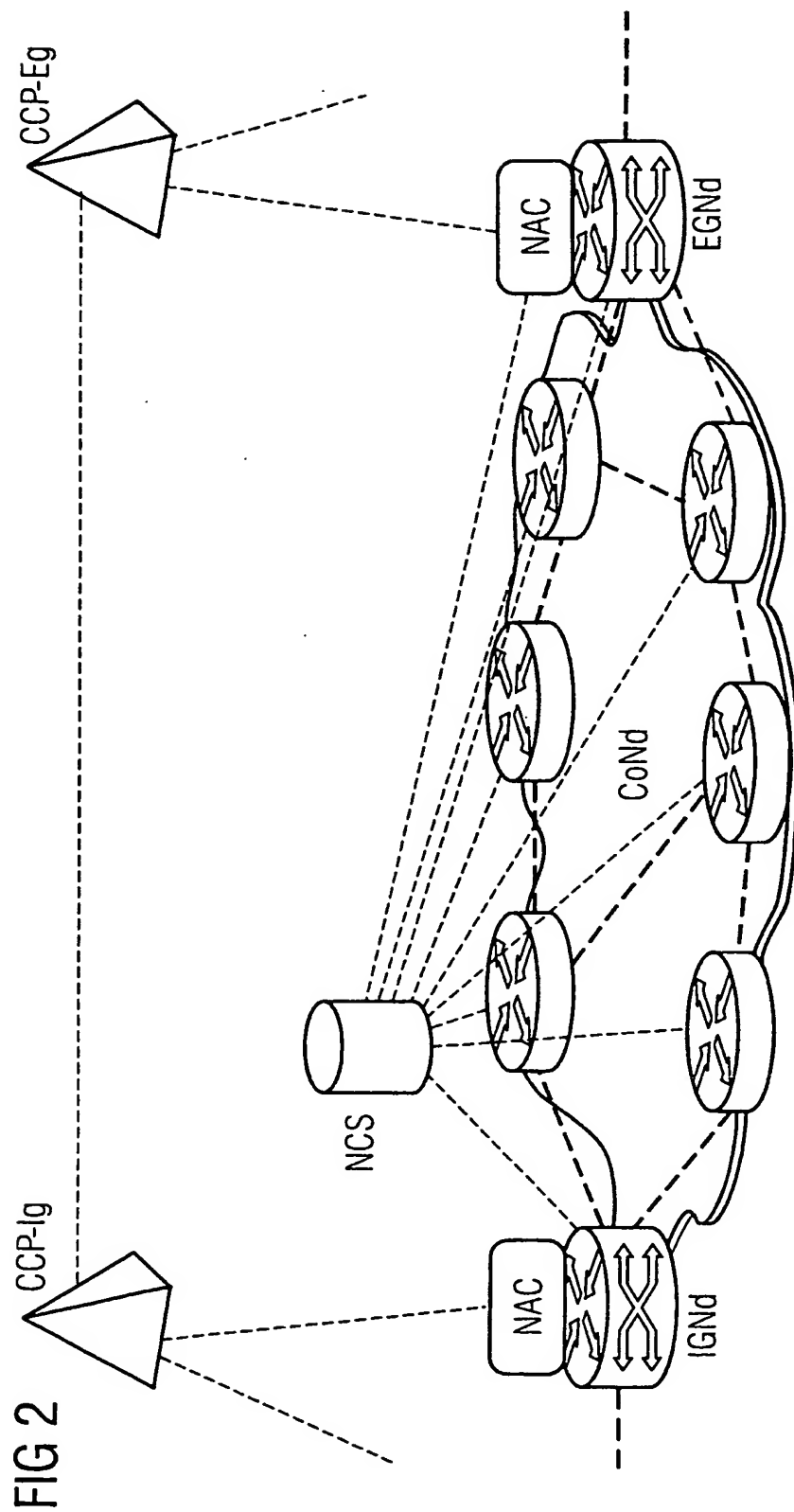
21

18. Randknoten zur Verwendung in einem paketorientierten, verbindungslosen Netz, wobei
- das Netz Mittel zur Durchführung einer Zulässigkeitsprüfung am Netzeingang oder am Netzausgang für die Übertragung eines durch das Netz zu leitenden Verkehrsstrom einer Prioritätsklasse aufweist, und
 - der Randknoten mit Mitteln zur Durchführung einer Zulässigkeitsprüfung am Netzeingang oder am Netzausgang für die Übertragung eines durch das Netz zu leitenden Verkehrsstrom einer Prioritätsklasse ausgestattet ist.
19. Randknoten nach Anspruch 18,
- mit Mitteln zur Überwachung von in dem Netz angemeldeten Verkehrsparametern.
20. Server zur Verwendung in einem paketorientierten, verbindungslosen Netz, wobei
- das Netz Mittel zur Durchführung einer Zulässigkeitsprüfung am Netzeingang oder am Netzausgang für die Übertragung eines durch das Netz zu leitenden Verkehrsstrom einer Prioritätsklasse aufweist, und
 - der Server mit Mitteln zur Durchführung einer Zulässigkeitsprüfung am Netzeingang und am Netzausgang für die Übertragung einer durch das Netz zu leitenden Gruppe von Datenpaketen einer Prioritätsklasse ausgestattet ist.
21. Server nach Anspruch 20,
- mit Mitteln zur Überwachung von in dem Netz angemeldeten Verkehrsparametern.

FIG 1

Projekt KING-Architectural Principle 1





3/4

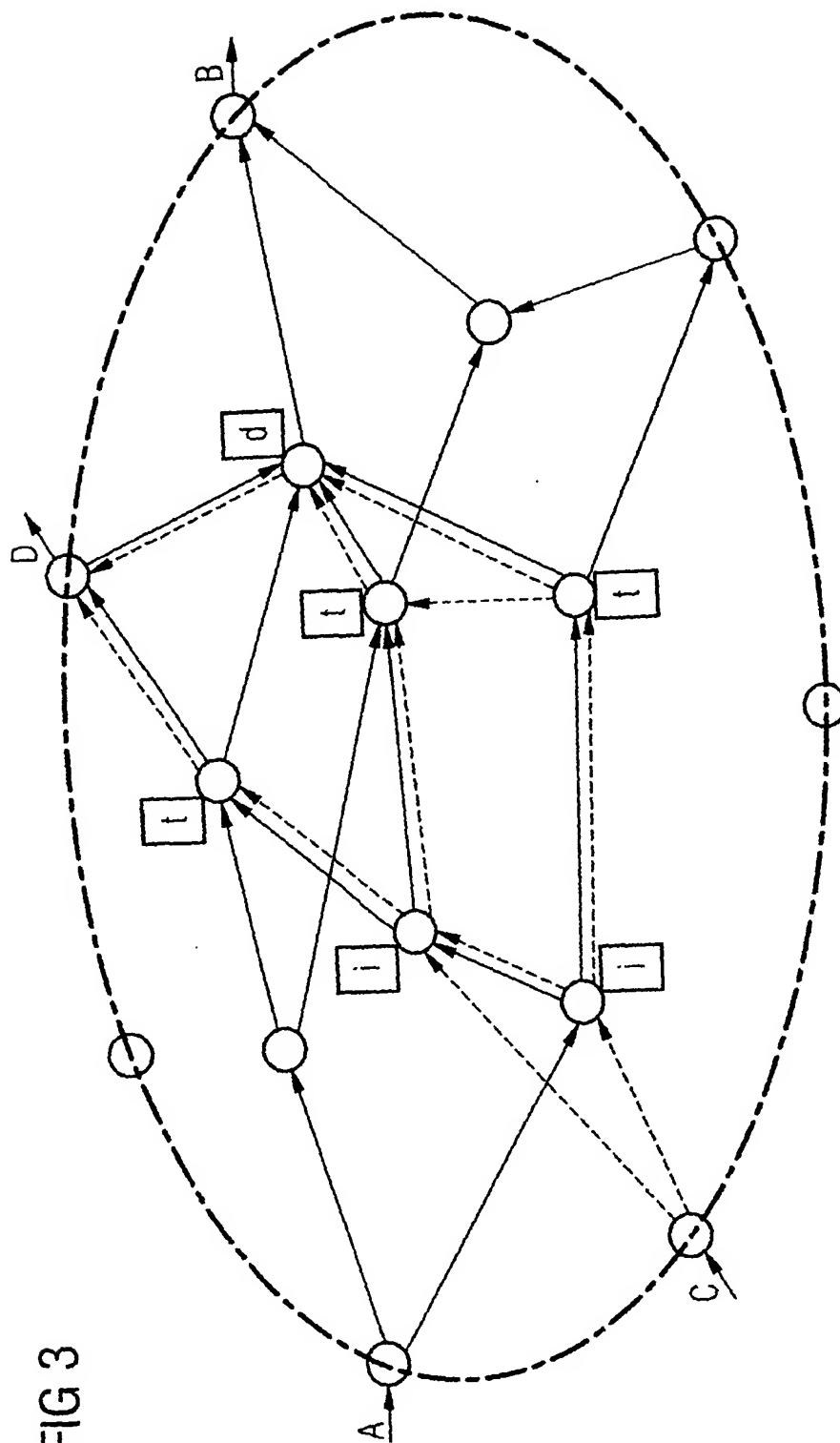
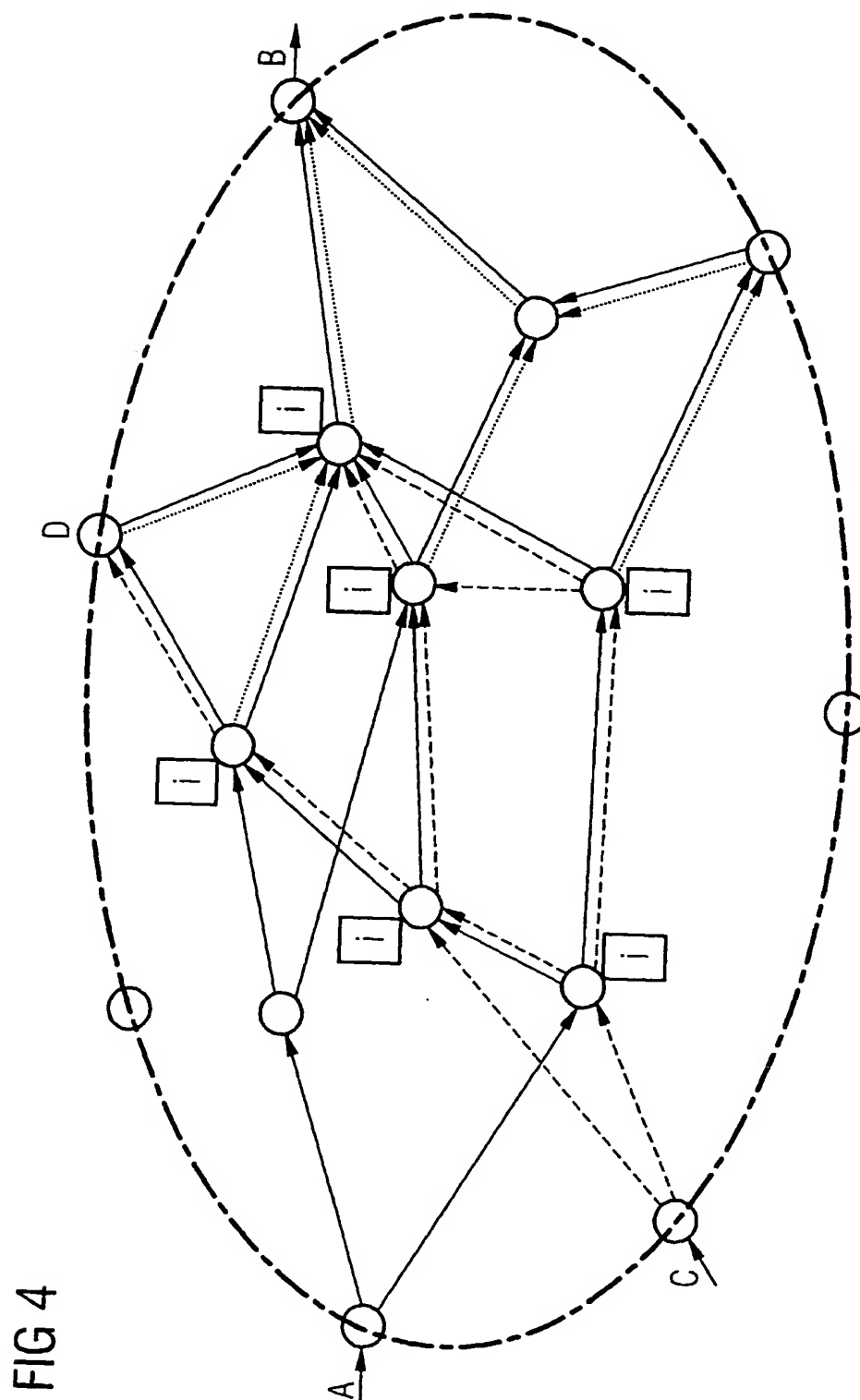


FIG 3



THIS PAGE BLANK (USPTO)

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record.

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)